**Al-Rafidain J Med Sci. 2026;11(1):143-145.**
**DOI:** https://doi.org/10.54133/ajms.v11i1.3147

**Editorial Letter**

AJMS
Online ISSN (3219-2789)

## Blockchain and Digital Healthcare: Promised Innovation or an Unfinished Revolution?

Valentino Natoli[1]*, Antonio Tammacco[2], Francesco Mileti[3], Vincenzo Natoli[4]
[1]*Department of Dentistry, School of Biomedical and Health Sciences, European University of Madrid, 28670 Madrid, Spain;* [2]*Innovation Manager According to the Standard UNI 11814, Think Next Srl, Molfetta 70056, Italy;* [3]*Department of Pediatrics, "Umberto I" Hospital, Fasano, (BR), Italy;* [4]*Private Dental Practice, 72015 Fasano, Italy*
Received: 1 June 2026; Accepted: 3 July 2026

****Corresponding author***: Valentino Natoli, Department of Dentistry, School of Biomedical and Health Sciences, European University of Madrid, 28670 Madrid, Spain; Email: valentinonatoliodn@gmail.com
***Article citation***: Natoli V, Tammaco A, Mileti F, Natoli V. Blockchain and Digital Healthcare: Promised Innovation or an Unfinished Revolution? *Al-Rafidain J Med Sci.* 2026;11(1):143-145. doi: https://doi.org/10.54133/ajms.v11i1.3147


Dear Chief Editor,

The digital transformation of healthcare is one of the most urgent and strategic challenges facing modern healthcare systems today. In this context, blockchain technology is often cited as a potential solution to issues of security, transparency, and clinical data management. But how ready is this technology to support the demands of a modern healthcare system? [1]. The term "blockchain" first appeared in 2009 in the source code of Bitcoin, created by Satoshi Nakamoto. Literally meaning "chain of blocks," it refers to a digital structure composed of distributed, interconnected ledgers that are immutable and verifiable through shared consensus mechanisms. Any information entered into the chain cannot be modified without the network's approval, a feature that makes blockchain a particularly attractive technology for all sectors where data security and reliability are paramount [2]. Among these, healthcare certainly plays a central role. Hospitals, laboratories, doctors, and patients handle enormous amounts of sensitive information on a daily basis, which must be protected from unauthorized access but, at the same time, easily shared among authorized professionals. Blockchain promises just that: a decentralized system that can guarantee traceability, interoperability, and security without depending on a single central authority [3]. The idea of building a connected healthcare ecosystem, where clinical data follows the patient securely and in real time, is an extremely compelling prospect. Thanks to decentralization, blockchain could improve collaboration among healthcare facilities, reduce administrative errors, and strengthen citizens' trust in the digital management of their medical information [4]. Crucially, the added value of blockchain in healthcare does not lie in data storage alone—a task a conventional encrypted database could also perform—but in its programmable layer: smart contracts. These self-executing programs allow access rules to be enforced automatically and verifiably: a patient may grant or revoke a given clinician's access to a specific record, insurance reimbursements may be triggered when predefined clinical conditions are met, and every access to sensitive data can be written to an immutable audit trail. It is this combination of decentralized trust and executable logic, far more than immutability by itself, that genuinely distinguishes a blockchain from a traditional clinical information system [5]. However, behind the technological enthusiasm lie critical issues that cannot be ignored. The first major obstacle is scalability. A necessary premise is the distinction between public, permissionless blockchains (such as Bitcoin or the Ethereum mainnet) and permissioned or consortium blockchains (such as Hyperledger Fabric, R3 Corda, or Quorum). Healthcare implementations almost never rely on public chains; they adopt permissioned architectures, in which a known and authorized set of nodes validates transactions. This distinction is decisive, because it reshapes the very problems discussed below. Public permissionless networks in particular struggle to handle the enormous volume of data produced by the healthcare sector: medical records, diagnostic images, test results, and data from medical devices generate an ever-growing amount of information. Storing this content directly on the blockchain would, at present, be inefficient and costly. Permissioned networks ease part of this burden by relying on lightweight consensus mechanisms (BFT- or RAFT-based) instead of the energy-intensive proof-of-work used by public chains, yet they do not remove the underlying need to keep large clinical payloads off the ledger. Beyond throughput, the choice of consensus mechanism carries two further implications that are often overlooked. The first is environmental: the Proof-of-Work model of public chains is notoriously energy-intensive, whereas the Byzantine-fault-tolerant protocols typical of permissioned networks consume a negligible fraction of that energy, making them far better suited to a healthcare context increasingly held to sustainability standards. The second is governance: in a permissioned consortium the validating nodes are known, accountable entities—hospitals, health authorities, and research centers—rather than anonymous miners, which provides precisely the auditable chain of responsibility that clinical data governance requires. For this reason, many experts propose hybrid solutions, in which health data is stored off-chain—that is, outside the blockchain—leaving only the references and cryptographic digital fingerprints of the documents on the chain. This approach is a pragmatic choice that is sometimes said to weaken the principle of immutability. In reality, immutability is preserved: the cryptographic fingerprint (hash) anchored on-chain still guarantees tamper evidence. Should the off-chain document be altered in any way, its recomputed hash would no longer match the value recorded on the ledger, and the manipulation would be immediately detectable. What the hybrid model actually sacrifices is not immutability but the decentralized availability of the content itself, which continues to depend on the off-chain storage layer and its security and resilience guarantees [6]. Added to this are regulatory and organizational challenges. In Europe, the GDPR guarantees citizens the so-called "right to be forgotten," that is, the ability to have their personal data deleted. This feature appears to conflict with the immutable nature of the blockchain. Furthermore, the widespread adoption of this technology would require advanced digital infrastructure, stable connections, and IT skills that are not yet evenly distributed across Europe [7]. These tensions, however, are not insurmountable, and a growing body of work outlines concrete mitigations. Keeping personal data off-chain—as already noted—removes most personal information from the immutable layer in the first place. Where data must be anchored on-chain, cryptographic erasure (destroying the decryption key so that the ciphertext becomes permanently unintelligible) offers a functional equivalent of deletion, while redactable blockchains based on chameleon hashes allow authorized, auditable edits without forking the chain. The EU Blockchain Observatory and Forum has likewise observed that compliance depends not on the technology as such but on how it is deployed and that GDPR requirements are markedly easier to satisfy in permissioned networks than in public ones [8,9]. The digital divide is, in fact, another decisive factor. Without adequate training and support, there is a risk of creating innovative systems that are difficult for citizens to access. A further, more practical obstacle concerns the management of cryptographic keys. In the patient-centered model described above, the patient controls access to their records through a private key; yet if that key is lost or stolen, the consequences are severe—irreversible loss of access in the first case and exposure of sensitive data in the second. Robust key-recovery and custody mechanisms are therefore a precondition for any patient-owned architecture, and they remain among the least resolved usability challenges in the field [10]. Finally, a more fundamental limitation is the so-called oracle problem. The blockchain can render a datum immutable once it has been recorded, but it cannot guarantee that the datum was accurate at the moment of entry: an erroneous clinical value is simply made immutably erroneous. Trust is therefore not eliminated but displaced—from the ledger to the systems and actors that feed data into it. In healthcare, where decisions hinge on data integrity, this shifts much of the assurance burden onto the medical devices, laboratory systems, and human operators at the input boundary [11]. Yet, despite these limitations, blockchain continues to be considered one of the most promising technologies for the future of digital healthcare. The most intriguing prospects today come from its integration with artificial intelligence, the Internet of Things, and big data. The combination of these technologies could enable smart healthcare systems capable of analyzing clinical data in real time, supporting personalized diagnoses, and improving the efficiency of care. The real challenge, therefore, is not just about technology, but about the ability to build a sustainable, interoperable, and patient-centered model. Because blockchain alone cannot revolutionize healthcare: it requires investment, multidisciplinary expertise, adequate infrastructure, robust data-governance and key-management frameworks, reliable mechanisms for validating data at the point of entry, and above all, a clear political and organizational vision. Ultimately, blockchain is not yet a definitive solution to the problems of digital healthcare, but rather a promising opportunity that is still maturing. Its future will depend on the ability to transform theoretical potential into concrete tools that are truly useful for doctors, healthcare facilities, and citizens. Only then will we be able to understand whether this technology will truly be the cornerstone of future healthcare or merely an unfulfilled promise [12].

***Keywords***: Blockchain in medicine; Health care; Health insurance.

### Conflict of interests

The authors declared no conflict of interest.

### Funding source

The authors did not receive any source of funds.

### Data sharing statement

N/A

## REFERENCES

1. Hasselgren A, Kralevska K, Gligoroski D, Pedersen SA, Faxvaag A. Blockchain in healthcare and health sciences-A scoping review. *Int J Med Inform*. 2020;134:104040. doi: 10.1016/j.ijmedinf.2019.104040.
2. O'Donoghue O, Vazirani AA, Brindley D, Meinert E. Design choices and trade-offs in health care blockchain implementations: Systematic review. *J Med Internet Res*. 2019;21(5):e12426. doi: 10.2196/12426.
3. Sivasankari B, Varalakshmi P. Blockchain and IoT technology in healthcare: A review. *Stud Health Technol Inform*. 2022;294:277-278. doi: 10.3233/SHTI220455.
4. Omidian H. Synergizing blockchain and artificial intelligence to enhance healthcare. *Drug Discov Today*. 2024;29(9):104111. doi: 10.1016/j.drudis.2024.104111.

5. Dinc R, Ardic N. An evaluation of opportunities and challenges of blockchain technology in healthcare. *Br J Hosp Med (Lond)*. 2024;85(11):1-19. doi: 10.12968/hmed.2024.0355.
6. European Union Blockchain Observatory and Forum (2018). Blockchain and the GDPR. Thematic Report, 16 October 2018. European Commission. Available at: https://blockchain-observatory.ec.europa.eu/publications/blockchain-and-gdpr_en
7. Hylock RH, Zeng X. A blockchain framework for patient-centered health records and exchange (HealthChain): Evaluation and proof-of-concept study. *J Med Internet Res*. 2019;21(8):e13592. doi: 10.2196/13592.
8. Ateniese G, Magri B, Venturi D, Andrade ER. (2017). Redactable Blockchain – or – Rewriting History in Bitcoin and Friends. In 2017 IEEE European Symposium on Security and Privacy (EuroS&P) (pp. 111–126). IEEE. Available at: https://eprint.iacr.org/2016/757.pdf
9. Ali A, Ali H, Saeed A, Ahmed Khan A, Tin TT, Assam M, et al. Blockchain-powered healthcare systems: Enhancing scalability and security with hybrid deep learning. *Sensors (Basel)*. 2023;23(18):7740. doi: 10.3390/s23187740.
10. Li K, Lohachab A, Dumontier M, Urovi V. Privacy preservation in blockchain-based healthcare data sharing: A systematic review. *Peer Peer Netw Appl*. 2025;18(6):302. doi: 10.1007/s12083-025-02148-9.
11. Shahzad A, Chen W, Shaheen M, Zhang Y, Ahmad F. A robust algorithm for authenticated health data access via blockchain and cloud computing. *PLoS One*. 2024;19(9):e0307039. doi: 10.1371/journal.pone.0307039.
12. Caldarelli G. Understanding the blockchain oracle problem: A call for action. *Information*. 2020;11(11):509. doi: 10.3390/info11110509.